Syllabus du Mastère Spécialisé®
Cybersécurité des Opérateurs de Services Essentiels

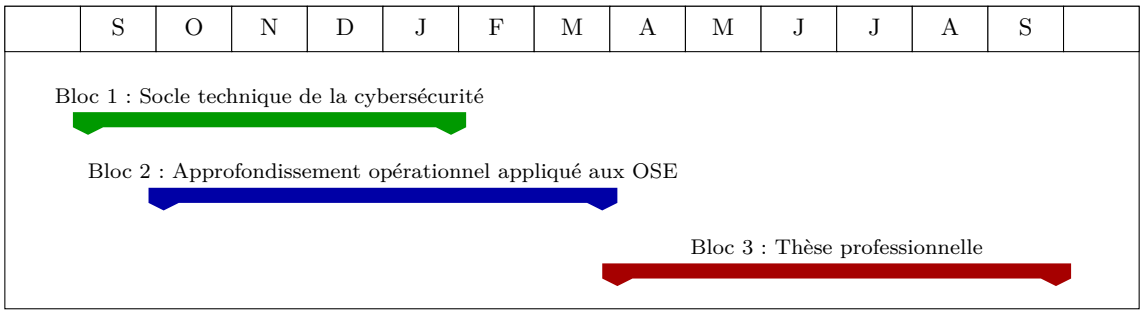
Code NSF 326 / CPF 248 343
Titre RNCP 7 n° 31043 : « Expert en Gouvernance de la Sécurité des Réseaux et des Systèmes »

La cybersécurité est aujourd'hui un enjeu essentiel pour nos sociétés modernes. Avec les évolutions des technologies (Cloud, Big Data, Internet des Objets, etc.) et des vecteurs d'attaque, les entreprises doivent disposer de spécialistes et d'experts en sécurité capables de protéger les informations sensibles et de suivre l'évolution des menaces et des vulnérabilités.

La situation a évolué récemment avec la réglementation européenne (NIS), qui impose désormais aux opérateurs de services essentiels de mettre en place des mesures de sécurité sur leurs systèmes d'information. C'est notamment aux personnels actuels et futurs de ces opérateurs que cette formation s'adresse.

Le mastère spécialisé « Cybersécurité des Opérateurs de Services Essentiels » est enregistré au registre national de la certification professionnelle en tant que titre de niveau 1, sous l'intitulé « Expert en Gouvernance de la Sécurité des Réseaux et des Systèmes » (titre n° 31043).

Découpage de la formation



Responsable : **Christophe Kiennert**
Maître de conférences en cybersécurité
Email : christophe.kiennert@telecom-sudparis.eu

1 Présentation et objectifs

Présentation

Les personnes concernées par ce programme peuvent être :
— professionnels opérateurs de services essentiels, désireux de se former à la cybersécurité ;
— professionnels de l'informatique, désireux de se former à la cybersécurité des OSE ;
— professionnels de la cybersécurité, désireux de se former aux aspects spécifiques aux OSE ;
— jeunes diplômés en informatique, désireux de se former à la cybersécurité.

Les pré-requis techniques sont :
— Réseaux TCP/IP
  — Adressage IP
  — Protocoles couches basses
  — Routage
  — Protocoles applicatifs
  — Notions sur les protocoles sécurisés
— Systèmes et développement
  — Architecture des ordinateurs
  — Notions sur les OS
  — Connaissances en particulier de Linux
  — Notions de programmation impérative
  — Connaissance d'un langage de scripts

Objectifs

L'objectif de cette formation est de répondre aux exigences de la gouvernance de la sécurité dans les entreprises avec une approche globale couvrant les aspects techniques, méthodologiques, organisationnelles et juridiques.

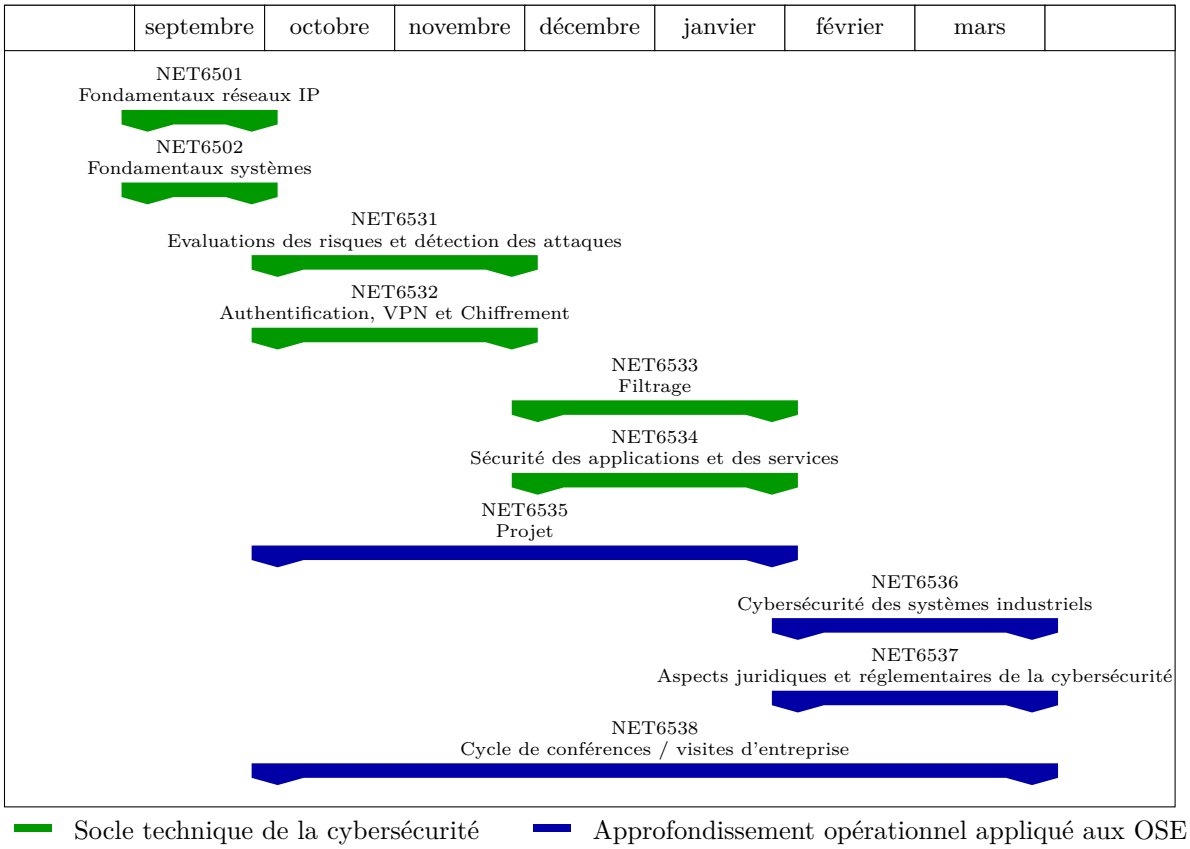
Elle permet d'apporter les connaissances nécessaires à l'élaboration et la mise en place d'un plan de sécurité destiné à la protection des ressources vitales de l'entreprise, contre les attaques internes et externes.

Compétences

Les compétences acquises au cours de cette formation permettront aux participants :
— de développer une capacité d'analyse et de restitution sur des problématiques de cybersécurité,
— de disposer des connaissances nécessaires pour concevoir et mettre en œuvre une architecture de sécurité,
— d'acquérir une connaissance pointue des aspects organisationnels, méthodologiques et juridiques de la cybersécurité, plus particulièrement dans le contexte des opérateurs de service essentiels,
— d'acquérir une expertise sur les pratiques opérationnelles des professionnels de la cybersécurité.

2 Contenu de la formation

Partie académique



Thèse professionnelle

À partir du mois d'avril, les étudiants partiront en thèse professionnelle, pour une durée de 5 à 6 mois.

Présentation du programme

Code	Intitulé du cours	Volume horaire [1]				Crédits ECTS
		Prés.	Proj.	TPers.	Total	
Socle technique de la cybersécurité						
NET6501	Fondamentaux réseaux IP	20		30	**50**	2
NET6502	Fondamentaux systèmes	20		30	**50**	2
NET6531	Evaluations des risques et détection des attaques	45		90	**135**	5
NET6532	Authentification, VPN et Chiffrement	45		90	**135**	5
NET6533	Filtrage	45		90	**135**	5
NET6534	Sécurité des applications et des services	45		90	**135**	5
Approfondissement opérationnel appliqué aux OSE						
NET6535	Projet	5	220		**225**	8
NET6536	Cybersécurité des systèmes industriels	45		90	**135**	5
NET6537	Aspects juridiques et réglementaires de la cybersécurité	30	15	90	**135**	5
NET6538	Cycle de conférences / visites d'entreprise	20	20	40	**80**	3
Thèse professionnelle		*5-6 mois*				30

1. Les volumes horaires correspondent au temps de cours en présentiel (Prés.), au temps dédié dans l'emploi du temps aux projets (Proj.), au temp de travail personnel estimé pour chaque module (TPers.), et au volume horaire total (Total).

2.1 NET6501 : Fondamentaux réseaux IP

Responsable : Patrick Maigron

Volume horaire : 20h en présentiel, 30h de travail personnel, soit **50h** au total

Crédits ECTS : 2 crédits ECTS

Période : septembre

Objectifs du cours et compétences acquises :

Il s'agit d'un bref module de présentation des notions fondamentales des réseaux IP. Les cours seront également l'occasion d'inclure quelques premières notions de sécurité.

Contenu détaillé du cours :

- Travaux pratiques de rappels sur les réseaux IP
- DNS et sécurité
- SMTP et sécurité

Méthodes et/ou moyens pédagogiques : Cours (9h) + TP (9h) + examen (2h)

Modalités d'évaluation : Examen

2.2 NET6502 : Fondamentaux systèmes

Responsable : Olivier Levillain

Volume horaire : 20h en présentiel, 30h de travail personnel, soit **50h** au total

Crédits ECTS : 2 crédits ECTS

Période : septembre

Objectifs du cours et compétences acquises :

Il s'agit d'un bref module de présentation des notions fondamentales en système. Les cours seront également l'occasion de tisser des premières notions de sécurité pertinentes sur les systèmes d'exploitation.

Contenu détaillé du cours :

- Travaux pratiques de rappels sur les systèmes Linux
- Travaux pratiques de rappels sur les systèmes Windows
- Modèle de sécurité Unix

Méthodes et/ou moyens pédagogiques : Cours(9h) + TP (9h) + examen (2h)

Modalités d'évaluation : Examen

2.3 NET6531 : Evaluations des risques et détection des attaques

Responsable : Grégory Blanc

Volume horaire : 45h en présentiel, 90h de travail personnel, soit **135h** au total

Crédits ECTS : 5 crédits ECTS

Période : octobre – novembre

Objectifs du cours et compétences acquises :

À l'issue de ce module, sur un cas d'étude de réseau informatique ou industriel simple, mais réaliste, l'étudiant pourra :

- identifier les risques, découvrir les vulnérabilités et évaluer la sécurité du réseau ;
- appréhender la démarche d'analyse de risque EBIOS et employer les outils d'audit d'un réseau.

Sur une application Web réaliste, l'étudiant est capable de mettre en oeuvre des techniques d'audit d'application Web et réaliser un rapport d'audit.

Quel que soit le contexte, l'étudiant aura acquis les compétences suivantes :

- expliquer le fonctionnement des centres de sécurité opérationnelle (SOC) et de réponse à incident (CERT) ;
- expliquer la méthodologie de la réponse à incident et inspecter partiellement des cas d'études.

Contenu détaillé du cours :
- Sécurité des réseaux : menaces et parades
- Méthodologies d'Analyse des Risques
- Audits techniques
- Réponse à incident
- Sécurité des systèmes industriels

Méthodes et/ou moyens pédagogiques : Cours intégré (42h) + examen (3h)

Modalités d'évaluation : TP noté + examen

2.4 NET6532 : Authentification, VPN et Chiffrement

Responsable : Maryline Laurent

Volume horaire : 45h en présentiel, 90h de travail personnel, soit **135h** au total

Crédits ECTS : 5 crédits ECTS

Période : octobre – novembre

Objectifs du cours et compétences acquises :

À l'issue du module, les étudiants pourront :
- mettre en œuvre les services d'authentification et de chiffrement, notamment sur des boitiers Stormshield et sur des systèmes Linux ;
- citer et décrire les mécanismes de gestion d'identité tels que le SSO (*Single Sign On*) et les infrastructures de clefs publiques (PKI, *Public Key Infrastructure* en anglais) ;
- pratiquer la génération et l'utilisation de certificats électroniques à l'aide de la librairie OpenSSL ;
- connaître les mécanismes utilisés dans les VPNs (*Virtual Private Networks*) ;
- configurer des VPNs basés sur IPsec, notamment sur des boitiers Stormshield et sur des systèmes Linux ;
- expliquer la cryptographie, discuter les algorithmes de chiffrement les plus couramment utilisés et appréhender les mécanismes avancés ;
- exprimer les bases et les enjeux de sécurité des protocoles associés aux nouveaux services.

Contenu détaillé du cours :
- Architecture et protocoles d'authentification (EAP, AAA)
- Solutions PKI et SSO (Single Sign On), protocoles d'authentification
- Cryptographie : mécanismes mathématiques et algorithmes, protocoles et applications
- VPN (Réseaux privés virtuels) et IPsec
- Mise en œuvre d'un VPN et du NAT
- Mise en œuvre de la génération et de l'utilisation de certificats électroniques
- Protocoles de Sécurité

Méthodes et/ou moyens pédagogiques : Cours intégré (42h) + examen (3h)

Modalités d'évaluation : TP noté + examen

2.5 NET6533 : Filtrage

Responsable : Olivier Paul

Volume horaire : 45h en présentiel, 90h de travail personnel, soit **135h** au total

Crédits ECTS : 5 crédits ECTS

Période : décembre – janvier

Objectifs du cours et compétences acquises :

À l'issue de ce module, les étudiants auront acquis les compétence suivantes :
- connaitre les problèmes que les systèmes de filtrage visent à résoudre ainsi que les mécanismes qui peuvent déployer dans un réseau ;
- expliquer le fonctionnement de ces mécanisme de filtrage ;
- dans le cadre d'une politique de sécurité donnée, être capable de comparer l'utilité des mécanismes et de sélectionner le plus approprié ;

— mettre en œuvre les mécanismes de filtrage (à base de routeurs, firewalls) en tenant compte d'une politique de sécurité.

Contenu détaillé du cours :

— Introduction aux problèmes de filtrage (cours, 2 heures)
— TP filtrage sur architecture éclatée Cisco IOS FW, AWS SG et NACL et proxy WAF sous AWS (TP, 6 heures)
— Problèmes et techniques de filtrage pour les couches 2, 2.5 (cours, 3 heures)
— TP filtrage au niveau 2, 2.5 (TP, 6 heures)
— Architectures des outils de filtrage (cours, 6 heures)
— NAT, Filtrage et applications multimédia (cours, 3 heures)
— TP NAT et VoIP (TP, 4,5 heures)
— Techniques de traitement des déni de service (cours, 4 heures)
— TP filtrage avancé sur architecture intégrée Checkpoint (TP, 9 heures)

Méthodes et/ou moyens pédagogiques : Cours (18h) + TP (25,5h) + examen (1,5h)

Modalités d'évaluation : TP noté + examen

2.6 NET6534 : Sécurité des applications et des services

Responsable : Olivier Levillain

Volume horaire : 45h en présentiel, 90h de travail personnel, soit **135h** au total

Crédits ECTS : 5 crédits ECTS

Période : décembre – janvier

Objectifs du cours et compétences acquises :

À la fin de ce module les étudiants devront :

— comprendre les problématiques de sécurité des applications informatiques et appréhender les principales stratégies de prévention et de résolution de ces problèmes ;
— expérimenter les méthodes d'injection de code dans les applications et les techniques permettant d'y résister ;
— comprendre les relations entre la sécurité des applications et l'établissement de réseaux de confiance en particulier pour les applications Java, et les distributions Linux ;
— comprendre les problématiques de sécurité associées à l'échange de documents ;
— comprendre le fonctionnement des virus et des anti-virus ;
— comprendre les interfaces entre les applications et le système d'exploitation (Linux / Windows + Active Directory).

Contenu détaillé du cours :

— Sécurité des applications en Java
— Sécurité Windows et Active Directory
— Virus et anti-virus
— Sécurité des documents
— Sécurité Linux
— Sécurité des développements

Méthodes et/ou moyens pédagogiques : Cours intégré (42h) + examen (3h)

Modalités d'évaluation : TP noté + examen

2.7 NET6535 : Projet

Responsable : Olivier Paul

Volume horaire : 5h en présentiel, 220h de projets, soit **225h** au total

Crédits ECTS : 8 crédits ECTS

Période : octobre – janvier

Objectifs du cours et compétences acquises :

À la fin du module, les étudiants peuvent :

- dégager une problématique associée à un sujet ;
- analyser l'état de l'art associé à cette problématique ;
- apporter une réponse d'ingénieur à cette problématique ;
- concevoir et réaliser un prototype répondant à cette problématique ;
- présenter de manière écrite et orale (sous la forme d'un rapport, d'un poster et d'une présentation orale) les résultats obtenus.

Contenu détaillé du cours :

Après une présentation des projets, les étudiants disposent d'un volume horaire important pour développer leur sujet et faire une restitution écrite et orale.

Les sujets sont proposés soit par des enseignants-chercheurs, soit par des industriels, qui jouent le rôle de tuteurs du projet pendant la durée du module.

Voici quelques exemples de projets :

- démonstrateur de canaux cachés réseau ;
- étude des normes et standards de la détection d'intrusion ;
- mise en œuvre d'un protocole basé sur du zero-knowledge dans la sécurisation d'une messagerie ;
- analyse de la sécurité NFC en pratique ;
- étude des attaques sur le réseau GSM avec OpenBTS ;
- étude de la résistance aux attaques des claviers virtuels javascript ;
- évaluation de la sécurité d'une application web ;
- analyse comportementale de malwares et génération de signatures.

Méthodes et/ou moyens pédagogiques : Projet en binôme

Modalités d'évaluation : Rapport + soutenance

2.8 NET6536 : Cybersécurité des systèmes industriels

Responsable : Joaquin Garcia Alfaro

Volume horaire : 45h en présentiel, 90h de travail personnel, soit **135h** au total

Crédits ECTS : 5 crédits ECTS

Période : février – mars

Objectifs du cours et compétences acquises :

Les compétences acquises durant ce module sont les suivantes :

- connaître les spécificités des systèmes industriels dans les infrastructures modernes ;
- savoir analyser les risques ;
- prendre en compte des mesures de protection pour les systèmes industriels.

Dans ce module, l'accent est mis sur l'instanciation des problématiques génériques à des secteurs d'activité concrets.

Contenu détaillé du cours :

- Cybersécurité des systèmes de transport ferroviaires
- Cybersécurité des systèmes de distribution d'énergie
- Cybersécurité des protocoles industriels
- Détection d'intrusions en environnement industriel
- Firmwares
- Sécurité des IoT

Méthodes et/ou moyens pédagogiques : Cours intégré (42h) + examen (3h)

Modalités d'évaluation : Examen

2.9 NET6537 : Aspects juridiques et réglementaires de la cybersécurité

Responsable : Hervé Debar

Volume horaire : 30h en présentiel, 15h de projets, 90h de travail personnel, soit **135h** au total

Crédits ECTS : 5 crédits ECTS

Période : février – mars

Objectifs du cours et compétences acquises :

Ce module a pour vocation de donner aux élèves une connaissance approfondie du panorama juridique et réglementaire en cybersécurité. Contrairement aux autres modules qui sont majoritairement techniques, ce module vise à développer les compétences juridiques et réglementaires nécessaires pour une bonne insertion professionnelle des étudiants dans l'écosystème européen de la cybersécurité.

Contenu détaillé du cours :

- Aspects économiques de la cybersécurité
- Intelligence économique
- Standardisation et réglementation NIS
- Certification
- Gestion de projets cybersécurité
- Framework CSF (*Cybersecurity Skills Framework*)

Méthodes et/ou moyens pédagogiques : Cours intégré (30h) + étude de cas en binôme

Modalités d'évaluation : Étude de cas + soutenance

2.10 NET6538 : Cycle de conférences / visites d'entreprise

Responsable : Hervé Debar

Volume horaire : 20h en présentiel, 20h de projets, 40h de travail personnel, soit **80h** au total

Crédits ECTS : 3 crédits ECTS

Période : octobre – mars

Objectifs du cours et compétences acquises :

- Connaître l'écosystème industriel des OSE
- Connaître l'état de l'art et les pratiques opérationnelles des professionnels du domaine

Contenu détaillé du cours :

Ce cycle de conférences et de visites d'entreprises sera organisé en parallèle de la scolarité.

Les étudiants participeront à l'organisation des conférences et visites. En particulier, ils présenteront les intervenants et les entreprises concernées.

L'évauation se fera sur un rapport collectif décrivant leur connaissance de l'état de l'art et des pratiques opérationnelles du domaine.

Méthodes et/ou moyens pédagogiques : Conférences / visites

Modalités d'évaluation : Rapport

3 Organisation pédagogique

3.1 Partie académique

Les tableaux suivant donne la répartition du volume horaire du MS Cybersécurité des Opérateurs de Services Essentiels. Ce volume est découpé en heures de cours en présentiel (cours magistral, travaux dirigés et travaux pratiques), en heures de projet (créneaux réservés dans l'emploi du temps) et en heures de travail personnel.

Bloc 1 : Socle technique de la cybersécurité

Code	Intitulé du cours	Volume horaire			
		Présentiel	Projets	T. Pers.	Total
NET6501	Fondamentaux réseaux IP	20		30	**50**
NET6502	Fondamentaux systèmes	20		30	**50**
NET6531	Evaluations des risques et détection des attaques	45		90	**135**
NET6532	Authentification, VPN et Chiffrement	45		90	**135**
NET6533	Filtrage	45		90	**135**
NET6534	Sécurité des applications et des services	45		90	**135**
Volumes horaires pour le bloc		220		420	**640**

Bloc 2 : Approfondissement opérationnel appliqué aux OSE

Code	Intitulé du cours	Volume horaire			
		Présentiel	Projets	T. Pers.	Total
NET6535	Projet	5	220		**225**
NET6536	Cybersécurité des systèmes industriels	45		90	**135**
NET6537	Aspects juridiques et réglementaires de la cybersécurité	30	15	90	**135**
NET6538	Cycle de conférences / visites d'entreprise	20	20	40	**80**
Volumes horaires pour le bloc		100	255	220	**575**

3.2 Mission en entreprise

À l'issue du premier semestre académique, la formation comprend une mission en entreprise obligatoire, d'une durée de 5 à 6 mois à temps plein minimum.

La mission en entreprise donne lieu à la rédaction d'une thèse professionnelle, qui consiste en un rapport synthétisant de manière détaillée et organisée le travail effectué au cours de la mission. La rédaction de ce rapport est par ailleurs suivie d'une soutenance, qui consiste en une présentation des travaux pendant une durée de 30 minutes, suivie d'une séance de questions-réponses de 15 minutes.

La mission en entreprise est sanctionnée par quatre notes :

— La note attribuée par le tuteur en entreprise sur le travail réalisé
— La note attribuée par le tuteur en entreprise sur la thèse professionnelle
— La note attribuée par le tuteur académique sur la thèse professionnelle
— La note attribuée par le jury sur la soutenance

La mission en entreprise est validée si la moyenne de ces quatre notes est supérieure ou égale à 10 sur 20.

3.3 Validation des connaissances

Le système d'évaluation des connaissances est spécifique à chaque module et précisé dans les différentes fiches modules.

La validation d'un module est acquise si la note finale obtenue pour ce module est supérieure ou égale à 10 sur 20.

L'obtention du diplôme est conditionnée par la validation de tous les modules composant la formation et de la mission en entreprise, suivant les modalités décrites dans la section précédente.